International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE www.irjcs.com

Secure Energy Optimization with Data Integrity Assurance in Wireless Sensor Networks – A Survey

Kantharaju .H.C[#1], Dr. K.N. Narasimha Murthy[#2]
[#1]*Assistant Professor, Department of CSE, Vemana Institute of Technology, Bengaluru, KA, India*
[#2]*Professor, Faculty of Engineering, Christ University, Bengaluru, KA, India*

Abstract *- **WSNs are very much in need for an integrated secure and efficient energy and power optimization mechanism due to the increased number of applications each day. Therefore, considering most of the existing techniques where energy optimization and security are provided in separate protocols, we design a new protocol with novel security provision with data integrity for the communicating data along with the energy optimization. The proposed Secure Energy Optimization with Data Integrity Assurance (SEODIA) will provide better energy efficiency and security of data compared to existing approaches.***

Keywords: ***Wireless Sensor Network, Secure Energy Optimization, Data Integrity Assurance.***

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have been widely considered as one of the most important technologies for the twenty-first century. A typical Wireless Sensor Network (WSN) consists of a large number low cost, multi-functional sensor nodes typically operate on limited battery power and are deployed to monitor an area of interest. These sensor nodes are typically small in size with inbuilt micro-controllers and radio transceivers. Thus, sensor nodes have the ability to sense external events, process the sensed data and transmit it. WSNs are widely used for environmental condition monitoring, security surveillance of battle-fields, wildlife habitat monitoring, etc. A WSN has the following characteristics:

- *Dense Node Deployment: Sensor nodes are usually densely deployed in an area to be monitored. The number of sensor nodes in a sensor network is usually higher than that of a MANET*
- *Limited Energy Resources: Sensor nodes are usually powered with small batteries. In certain applications, they are deployed in a harsh or hostile environment, where it would be very difficult or even impossible to replace or recharge the node batteries.*
- *Self and Auto-Configuration of Nodes: Sensor nodes could be randomly deployed without careful planning. Once deployed, sensor nodes could autonomously configure the network.*
- *Application Specific Nodes: Sensor networks are usually application specific. Sensor nodes are designed and deployed for a specific application. Thus, the design requirements of a sensor network could change based on the application requirement.*
- *Frequent Topology Change: In a sensor network, the topology could change frequently due to node failure, energy depletion or channel fading.*
- *Coverage Area and Data Redundancy: In most sensor network applications, sensor nodes are densely deployed in a region of interest. Therefore, there might be a possibility that more than one sensor node is monitoring a sensing area. Thus, the data sensed by multiple sensor nodes may have a certain amount of correlation or redundancy.*

II. LITERATURE SURVEY

A. AUTHENTICATION SCHEME BASED POWER OPTIMIZATION TECHNIQUE

The main use of authentication Scheme based power optimization technique is for draining the injected invalid data from wireless sensor network and save the power in WSN. In this technique Message Authentication code is used. Message authentication code (MAC) provides knowledge to the recipient of the message which came from the expected sender and has not been altered in transit. This scheme achieves high reliability and high en-routing filtering probability with multi report. This scheme is simple and effective, that it could be used in mobile sensor node authentication scenarios.

B. NEW ANT COLONY OPTIMIZATION (NACO) TECHNIQUE

The ACO based routing algorithm is used to find the minimum route of nodes in wireless sensor networking the basis of pheromone updating. NACO is very effective for communication from source node to destination node. NACO is reliable, nature-inspired routing algorithm which is partly based on the efficient Max-Min algorithm and it is suitable for flexible

structure of wireless sensor networks. This new routing scheme performs generally not worse than other standard routing algorithm, and in some occasions, it outperforms than min-hop algorithm.

C. USING DATA MINING TECHNIQUE (DECISION TREE ALGORITHM) IN ZRP PROTOCOL

Zone Routing Protocol (ZRP) is the combination of two protocols (proactive and reactive). ZRP was proposed to minimized the control overhead of PRP (proactive routing protocols) and decrease the latency caused by route discovery in RRP (reactive routing protocols). ZRP explains a zone around each node formation of the node's neighbourhood. The first protocol to be part of ZRP is the Intra zone Routing Protocol (IARP). This protocol is used by a node to communicate with the interior nodes of its zone and as such is limited by the zones radius, the global reactive routing component of the ZRP, the Inter zone Routing Protocol (IERP), takes advantage of the known local topology of a node's zone and, using a reactive approach enables communication with nodes in other zones.

D. MINIMUM TOTAL TRANSMISSION POWER ROUTING (MTPR)

MTPR protocol focuses on end-to-end energy efficiency. Generally, the route selected for conserving energy is the shortest distance path or minimum hop path, the end-to end shortest path naturally leads to conservation of energy in transmission. In a non-partitioned network, there exists at least one path for communication with any other node. So theoretically, any node can reach any other node in the network through a random forwarding path. However, the energy consumption along different paths differs, due to its dependence on variations of distance between directly communicating nodes and noise interference levels.

E. MINIMUM BATTERY COST ROUTING (MBCR)

Though the transmission power is an important metric to consider, if multiple minimum total power paths pass through some common node, then this common node will soon experience battery exhaustion. MTPR has a drawback in violating fair distribution of power consumption among nodes. It does not reflect the lifetime of individual nodes. This indicates that, as an alternative, node's residual energy can be used as a cost metric in route selection. MBCR is such a scheme that minimizes the path battery cost so as to maximize the total network life time. The cost function f in MBCR is defined such that the lower the remaining battery capacity c of a node i, the more reluctant the node is to receive and forward the packet.

F. ENERGY AWARE ROUTING (EAR)

This protocol clearly aims to increase the network lifetime of a network. It is similar to directed diffusion protocol but instead of using or enforcing single dedicated path at higher rates, it maintains a set of paths. Probability factor is the metric used for deciding a path. Probability of a path decides how much that path is energy efficient.

G. HYBRID ENERGY EFFICIENT DISTRIBUTED CLUSTERING- HEED

HEED was designed to select different cluster heads based on the amount of energy that is disseminated in relation to a neighboring node. HEED aims at increasing network life-time by uniformly distributing energy consumption, terminating the clustering process within a constant number of iterations/steps, minimizing control overhead and producing well-distributed cluster heads and compact cluster.

H. THRESHOLD SENSITIVE ENERGY EFFICIENT SENSOR NETWORK TEEN

In this protocol, a node keeps on monitoring the network continuously but enters the transmission mode only when a certain specified threshold is reached. There are two types of thresholds: hard threshold and soft threshold. Whenever, hard threshold is reached, the nodes recollect data and enter the transmission mode and send the sensed data to the cluster head. The drawback of this protocol is that if the thresholds broadcasted are not received, then sensed data will not be transmitted.

I. ACTIVE QUERY FORWARDING IN SENSOR NETWORK-ACQUIRE

ACQUIRE is a data centric approach used for querying named data. It has the edge in answering specific types of queries, called one-shot complex queries for replicated data. ACQUIRE query (i.e., interest for named data) has its subpart in the form of sub queries for which several important sensors provide the required responses. Each sub-query is answered based on the currently stored data at its relevant sensor. ACQUIRE allows a complex query to be injected into the network to be forwarded stepwise through a sequence of sensors.

J. SENSOR MAC-SMAC

SMAC is based on periodic sleep listen schedules which are handled locally by the sensor network. All nearby nodes tend to form virtual clusters and then they share their common schedules. This means that nodes falling under two different clusters will awake in listening period of both the clusters. This results in more energy consumption as nodes wake up to two different schedules. The schedules are also required to be communicated to different nodes of virtual cluster which is accomplished by SYNC packets and time in which it is sent is known as synchronization period. A new and most prominent feature of SMAC is messaging passing through which a long message is sent in burst by dividing it into small messages. This helps in energy saving by using common overhead.

K. POWER AWARE MULTIPLE ACCESS PROTOCOL WITH SIGNALLING (PAMAS)

This protocol layout is similar to MACA with addition of separate signaling channel. PAMAS conserves the node battery power by efficiently and intelligently turning off nodes that are not actively transmitting and receiving packets. It uses same RTS-CTS follow up scheme but these RTS-CTS message exchange takes place on a channel different from the channel meant for data transmission, this channel is called as signaling channel. This signaling channel helps nodes to know when and for how long they can be turned off.

II. METHODOLOGY

The proposed methodology aims to provide energy conversation and Security of data.

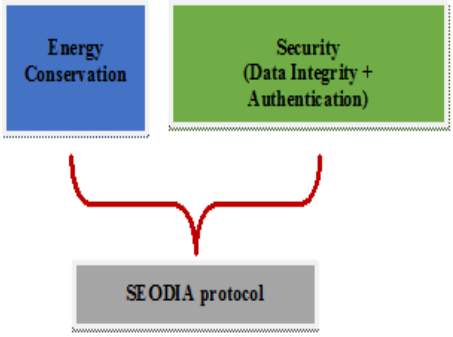

Fig. 3.1. Energy Conservation and Security Adaption in Wireless Sensor Network

A. ENERGY CONSERVATION

Energy conservation has to be achieved by managing the WSNs using hierarchical topology. Each cluster head node needs to predict the energy expenditure for the next cluster operation of the cluster. Let us consider that the N number of nodes are present and with M cluster groups. Therefore, there are possibly M cluster heads for every round of clustering. The energy expenditure for each node N can be measured using,

$E_N = ETx + ERx + Esen$

$E_{Mg} = m \times E_N$

$= m \times (ETx + ERx + Esen)$

Where,

ETx – Transmission Energy
ERx – Receiving Energy
Esen – Sensing Energy of a WSN node
m – number of members in each cluster g
E_{Mg} *– Energy of the gth cluster where g* ϵ *M*

B. SECURITY

There are two aspects of security in the network provided by both authentication and provision of security in the network. Each consecutive next node is authenticated using a novel authentication mechanism and a novel data security method.

III.CONCLUSION

Security and Energy Conservation are the most fundamental concerns in wireless sensor networks. Sensors can last for a few weeks using their batteries. The solution is to deploy some extra sensors and distribute the workload between nodes to increase the lifetime. In this case, some protocols are needed to schedule activation and deactivation of nodes while keeping the coverage and connectivity quality. The protocols maintaining the area covered are often referred to as coverage protocols while connectivity protocols guarantee the communication quality between nodes. A novel Security Energy Optimization and Security aspects are necessary in Wireless Sensor Networks to serve the environment better.

REFERENCES

[1]. Singh, Mukul Pratap, and Kunal Gupta. “Draining injected invalid data for efficient bandwidth consumption using authentication scheme in WSN.” International Journal of Scientific and Research Publications: 713.
[2]. Singha, Mukul Pratap, Ashish Kotsa, and Kunal Guptaa. "Reduction of Power using new ACO (Ant Colony Optimization) in Wireless Sensor Network." (2013).
[3]. Singh, Mukul Pratap, and Kunal Gupta. "Techniques of Power Optimization for Wireless Sensor Network." International Journal of Computer Applications 66.3 (2013).
[4]. Toh, C.-K.: Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks. IEEE Communications Magazine 39, 138–147 (2001).
[5]. Mahfoudh, Saoucene, and Pascale Minet. "Energy-aware routing in wireless ad hoc and sensor networks." Proceedings of the 6th International Wireless Communications and Mobile Computing Conference. ACM, 2010.
[6]. Younis, Ossama, and Sonia Fahmy. "HEED: a hybrid, energy efficient, distributed clustering approach for ad hoc sensor networks." Mobile Computing, IEEE Transactions on 3.4 (2004): 366-379.
[7]. Manjeshwar, Arati, and Dharma P. Agrawal. "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks." Parallel and Distributed Processing Symposium, International. Vol. 3. IEEE Computer Society, 2001.
[8]. N. Sadagopan, B. Krishnamachari, A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks". 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003, Pp. 149- 155, 11 May 2003.
[9]. S. Singh and C.S. Raghavendra, PAMAS: Power aware multi-access protocol with signaling for ad hoc networks, ACM SIGCOMM Computer Communication Review, Volume 28 Issue 3, July 1998.